For problems 0 and 1, see last week's solutions.

2) In the Euclidean algorithm, each remainder $r_i$ is a non-negative integer smaller than the previous one. It follows that the $r_i$'s must eventually reach 0 (it would take an inductive argument to make this rigorous.)

We know that each $r_{i+1} < r_i$. If $r_{i+1} \leq \frac{r_i}{2}$, then we have $r_{i+2} < r_{i+1} \leq \frac{r_i}{2}$ as well. On the other hand, if $r_{i+1} > \frac{r_i}{2}$, then the next step in the Euclidean algorithm is

$$r_i = 1 \cdot r_{i+1} + r_{i+2}$$

where $r_{i+2} = r_i - r_{i+1} < \frac{r_i}{2}$.

Either way, $r_{i+2} < \frac{r_i}{2}$. This means that the Euclidean algorithm ends in at most $2 \log_2 b$ steps.

This is very fast, for example it is much faster than any known algorithm to compute the prime factorization of $b$.
(Ask in class if you want to know more about computing time.)

3) If $d | a$ and $d | b$, then $d | r_n$.

pf: We can show that $d$ divides all $r_k$ by induction on $k$.
Base Case: $k=1$: If $d | a$ and $d | b$, then $d | a - bq_1 = r_1$.
Inductive Step: We make two inductive assumptions: that $d | r_{k-1}$ and that $d | r_k$. It follows immediately that $d | r_{k-1} - r_k q_{k+1} = r_{k+1}$, completing the induction.

Note: Making two inductive assumptions is a slightly different form of inductive proof. We really ought to have two base cases in this proof, e.g. we could start by setting $r_0 = b$. 
4) \( r_n | a \) and \( b \).

pf: We first show by reverse-induction on \( k \) that \( r_n \) divides all the other \( r_k \)'s, and then conclude that \( r_n | a \) and \( r_n | b \).

There are two base cases: \( r_n | r_0 \), and \( r_n | r_{n-1} = q_{n+1} r_n \).

Now suppose that \( r_n | r_{k+1} \) and \( r_n | r_k \). It follows that \( r_n | r_k \) since \( r_{k+1} = r_k \cdot q_{k+1} + r_{k+1} \). This proves that \( r_n | r_k \) for all \( k \), by reverse induction.

Finally, \( r_n | b \) since \( b = q_2 \cdot r_1 + r_2 \), and \( r_n | a \) since \( a = q_1 \cdot b + r_1 \).

5) There is an integer solution \( (x, y) \) to \( ax + by = r_n \).

pf: We show by induction on \( k \) that there is an integer solution \( (x_k, y_k) \) to \( ax_k + by_k = r_k \) for all \( k \).

Again, there are two base cases. For \( k = 1 \), let \( x_1 = 1 \), \( y_1 = -q_1 \), so \( ax_1 + by_1 = a - bq_1 = r_1 \).

For \( k = 2 \), let \( x_2 = -q_2 \), \( y_2 = q_1 q_2 + 1 \), so \( ax_2 + by_2 = -q_2 \cdot 1 + q_1 q_2 b + b = b - q_2 (a - bq_1) = b - q_2 r_1 = r_2 \).

For the inductive step, assume \( ax_{k-1} + by_{k-1} = r_{k-1} \) and \( ax_k + by_k = r_k \).

Then \( r_{k+1} = r_{k-1} - q_{k+1} r_{k-1} = ax_{k-1} + by_{k-1} - q_{k+1} ax_k - q_{k+1} by_k \).

So let \( x_{k+1} = -q_{k+1} x_k + x_{k-1} \), \( y_{k+1} = -q_{k+1} y_k + y_{k-1} \).

This completes the induction, showing that \( r_n \) can be expressed as \( ax + by \).

Problems 6-8 are a compilation of many previous results, showing that the four definitions of the greatest common divisor given in class make sense and are equivalent. You may use these definitions interchangeably from now on. If you have questions about them, please ask in class.
9) Suppose we have an integer $p > 1$ with the property that whenever $x$ and $y$ are integers and $p \mid xy$, then $p \mid x$ or $p \mid y$.

   Proof: This is a consequence of the definition of a prime.
   If $p$ is composite, then there are integers $1 < x, y < p$ such that $x \cdot y = p$. In this case $p \mid xy$ but $p$ does not divide $x$ or $y$.
   If there are no such integers $x$ and $y$, then $p$ must be prime.

10) Converse of 9: If $p$ is prime and $p \mid xy$, then $p \mid x$ or $p \mid y$.

   Proof: Assume $p$ is prime and $p \mid xy$ but $p \nmid x$. We will prove $p \mid y$.
   Since $p$ is a prime and does not divide $x$, the greatest common divisor of $p$ and $x$ is 1. By our past work on the g.c.d., this means that there are integers $m, n$ such that $pm + xn = 1$.
   Multiply both sides by $y$: $pmy + xyn = y$.
   Now $p$ divides $pmy$, and it divides $xyn$ because it divides $xy$, so we conclude that $p$ divides $y$.

11) Any integer $n > 1$ is a product of primes.

   Proof: Base Case: $n = 2$ is prime.

   Inductive Step: This problem is best solved by strong induction (see problem set 1, problem 11). We will assume that the integers between 1 and $k$ all have prime factorization, and prove that $k$ does also.
   There are two possibilities: if $k$ is prime, then it is its own factorization. Otherwise $k = xy$ with $1 < x, y < k$. By our inductive hypothesis, both $x$ and $y$ factor into primes. Multiplying these factorizations together provides a factorization of $k$. 
12) Suppose \( n > 1 \) is an integer and
\[
\begin{align*}
  n &= p_1 p_2 \ldots p_k = q_1 q_2 \ldots q_k,
\end{align*}
\]
where \( p_1 \) through \( p_k \) and \( q_1 \) through \( q_k \) are primes.

(a) Claim: Suppose \( p_i \mid q_1 q_2 \ldots q_k \) and \( p_i \) is prime. Then \( p_i \) divides some \( q_j \).
This is a generalization of problem (12) and can be proven using that problem.

An easy induction on \( k \). Since we are also assuming that the \( q_j \)'s are all prime, we can conclude that \( p_i = q_j \) for some \( j \).

(b) & (c). Claim: \( k = 1 \) and the \( p_i \)'s can be matched up with the \( q_i \)'s.

Proof: Induction on \( k \).

Base case: If \( k = 1 \), so \( p_1 = q_1 q_2 \ldots q_k \), since \( p_1 \) is prime, the
right side of the equation must be prime as well, so \( k = 1 \) and \( p_1 = q_1 \).

Inductive step: Given \( p_1 p_2 \ldots p_{k+1} = q_1 q_2 \ldots q_{k+1} \), by part (a)
\( p_1 = q_j \) for some \( j \), and we might as well assume \( j = 1 \).

Cancelling this factor on both sides gives \( p_2 p_3 \ldots p_{k+1} = q_2 q_3 \ldots q_{k+1} \).

By inductive hypothesis, \( k+1 = k+1 \), and all the remaining \( p_i \)'s can
be matched up with the \( q_i \)'s.

This completes the proof that prime factorization is unique.

13) \( \sqrt{2} \) is irrational.

Proof by contradiction: Suppose \( \sqrt{2} = \frac{p}{q} \), for \( p \) and \( q \) integers.

Then \( \frac{p^2}{q^2} = 2 \), so \( p^2 = 2q^2 \). We examine the prime factorization
of each side of this equation. \( p^2 \) must be divisible by an even power
of \( 2 \), while \( 2q^2 \) must be divisible by an odd power of \( 2 \).

This would contradict the law of unique prime factorization.